

What Is Claimed Is:

1 1. A method of producing at least one alert indication
2 based on a number of events derived from an enterprise
3 comprising:

4 providing a plurality of enterprise device outputs, at
5 least a portion of the outputs having different formats, each
6 output containing an event relating to an enterprise device;

7 translating each output into a common format event,

8 adding knowledge to the common format event using
9 knowledge base table files to generate a knowledge-containing
10 common format event; and

11 applying one or more rules from a set of rules to the
12 knowledge-containing common format event to generate the alert
13 indication.

14 2. The method of claim 1, wherein the common format event
15 contains at least a generic description of a specific event
16 occurring as part of each device output.

17 3. The method of claim 1, wherein generating the
18 knowledge-containing common format event further comprises
19 comparing the common format event for each network device to a
20 number of knowledge base table entries contained in a knowledge
21 base table, wherein knowledge is added from one or more of the

6 knowledge base table entries when a match between the translated
7 common format event and the entry in the knowledge base table is
8 made.

1 4. The method of claim 1, wherein the enterprise devices
2 are selected from the group consisting of a server, a firewall, a
3 modem, a work station, a router, a remote machine, an intrusion
4 detection system, an identification and authentication server,
5 network monitoring and management systems, network components,
6 and one or more combinations thereof.

7 5. The method of claim 1, wherein the translating step
8 further comprises:

9 matching data values in the device output with a signature
10 specification for each enterprise device, the signature
11 specification containing:

12 a number of signatures;

13 a first location identifier for each signature; and

a first key;

wherein the signature is a listing of names found in
the device output, the first location identifier
determines the method used to locate the name in the
device output, and the first key determines where to
locate the name in the device output;

14 identifying a message type from a plurality message types
15 for each enterprise device based on the device output as part of
16 the translated common format event;
17 producing the remainder of the translated common format
18 event in argument name and argument value pairs using an argument
19 specification, the argument specification containing;
20 a listing of arguments;
21 a field type;
22 a second location identifier for each argument; and
23 a second key;
24 wherein each argument is a listing of argument names for
25 inclusion in the translated common format event, the field type
26 specifies the form of an argument value found in the device
27 output, the second location identifier determines the location of
28 each argument value, and the second key locates the argument
29 value in the device output to be displayed with the argument
30 name.

1 6. The method of claim 1, wherein the knowledge-containing
2 common format event comprises one or more names selected from the
3 group of a device alert, a generic alert, a threat severity, a
4 benign explanation, a recommended action, a common
5 vulnerabilities and exposure code, a conclusion, and a category
6 code, and a corresponding value for each name.

1 7. The method of claim 1, wherein one or more rules
2 determine when or whether the knowledge-containing common format
3 event is generated, and final rule-based additions content of
4 such generated events.

1 8. The method of claim 7, wherein the rule requires that
2 the each output occur a number of times over a period of time
3 before an alert indication is generated.

1 9. The method of claim 1, wherein the output is one of an
2 unauthorized login, an unauthorized physical entry, and an
3 attempt to bypass a firewall.

1 10. The method of claim 3, wherein the translating step
2 further comprises:

3 matching data values in the device output with a signature
4 specification for each enterprise device, the signature
5 specification containing:

6 a number of signatures;

7 a first location identifier for each signature; and

8 a first key;

9 wherein the signature is a listing of names found in
10 the device output, the first location identifier
11 determines the method used to locate the name in the
12 device output, and the first key determines where to
13 locate the name in the device output;

14 identifying a message type from a plurality message types
15 for each enterprise device based on the device output as part of
16 the translated common format event;
17 producing the remainder of the translated common format
18 event in argument name and argument value pairs using an argument
19 specification, the argument specification containing;
20 a listing of arguments;
21 a field type;
22 a second location identifier; and
23 a second key;
24 wherein each argument is a listing of argument names for
25 inclusion in the translated common format event, the field type
26 specifies the form of an argument value found in the device
27 output, the second location identifier determines the location of
28 each argument value, and the second key locates the argument
29 value in the device output to be displayed with the argument
30 name.

1 11. The method of claim 10, wherein the rule determines
2 when or whether the knowledge-containing common format event is
3 generated.

1 12. The method of claim 11, wherein the rule requires that
2 each output occur a number of times over a period of time before
3 an alert indication is generated.

1 13. The method of claim 1, wherein the alert indication
2 includes at least a text message describing the event contained
3 in the output of the enterprise device.

1 14. The method of claim 13, wherein a threat level is
2 included as part of the alert indication.

1 15. A system for producing at least one alert indication
2 based on a number of events derived from an enterprise
3 comprising:

4 a plurality of enterprise devices, each device capable of
5 producing an output;

6 a number of translation files, the translation files
7 allowing the output to be translated into a common format event;

8 a number of knowledge base table files, matching of the
9 common format event with one or more of the knowledge base table
10 files adding knowledge from the matched file to generate a
11 knowledge-containing common format event;

12 a number of rule files, the rule files governing generation
13 of the alert indication.

1 16. The system of claim 15, wherein the enterprise devices
2 are selected from the group consisting of a server, a firewall, a
3 modem, a work station, a router, a remote machine, an intrusion
4 detection system, an identification and authentication server,
5 network monitoring and management systems, network components,

6 and one or more combinations thereof, or any generator of data
7 streams on the computer network.

1 17. The system of claim 15, wherein the knowledge-
2 containing common format event comprises one or more names
3 selected from the group of a device alert, a generic alert, a
4 threat severity, a benign explanation, a recommended action, a
5 CVE, a conclusion, and a category code, and a corresponding value
6 for each name.

1 18. The system of claim 15, wherein the common format event
2 comprises a message, and a number of name and value pairs derived
3 from the output of the enterprise device.

1 19. The system of claim 17, wherein the rule files govern
2 at least the frequency of the generation of the alert indication.

1 20. The system of claim 19, wherein the common format event
2 comprises a message, and a number of name and value pairs derived
3 from the output of the enterprise device.

1 21. The method of claim 7, wherein the rule adds
2 information to the knowledge-containing common format event.

1 22. The system of claim 11, wherein the rule adds
2 information to the knowledge-containing common format event.